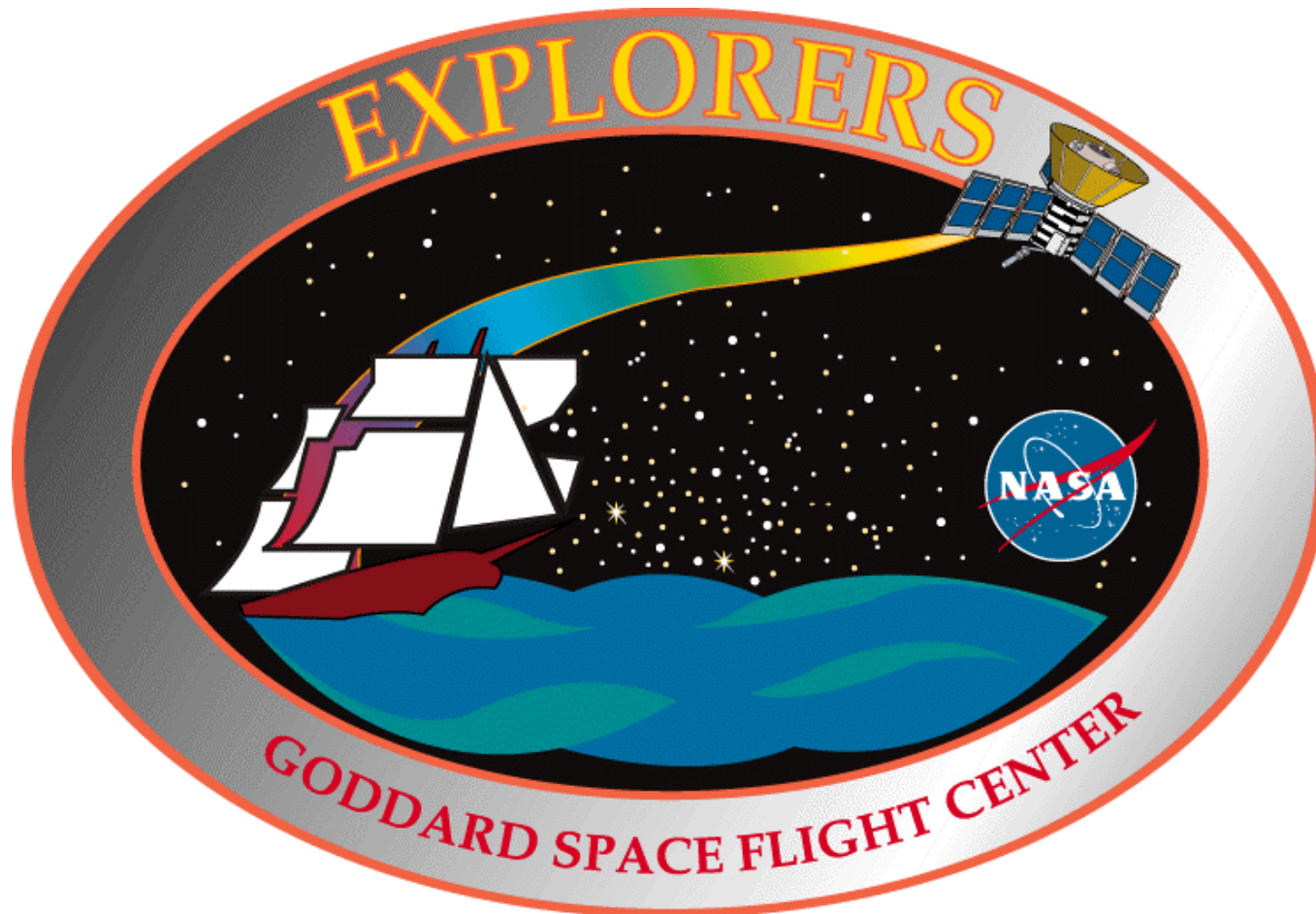# SMEX Kickoff Meeting Safety, Reliability, & Quality Assurance Handout

Rick Claffy, GSFC Code 410/303, X6-7866

May 1st, 2001 @ UMD

SMEX Kickoff Meeting SR&QA Handout

- **SR&QA effort is controlled by SMEX AO, EPL Reference Document #25.**
  - **Page 2, Par. 1.1 discusses EXP Program Office & PI joint effort to define best mix of roles and responsibilities for SR&QA execution.**
    - **Mission Definition & Requirements Agreement. (EPL Ref. #29)**
    - **Code 410/PI SR&QA Insight Agreement.**
      - **Becomes part of GSFC/PI Contract as a condition for confirmation.**
      - **Defines Early the Inter-Institutional Partnering Arrangement for SR&QA services.**
  - **Page 3, Par. 2.1 requires PIs to implement a product assurance program that is consistent with ISO 9000 series ANSI/ASQC Q9001-1994.**
    - **ISO registration not required, but compliance is expected with the Standard's sections where it makes good engineering and programmatic sense.**
    - **Program must meet SMEX Safety, Reliability, and Quality Assurance Requirements, as published with the AO.**
    - **Tailoring encouraged in most assurance technology areas, but …**
    - **The highly specialized discipline of System Safety, including the Range Safety effort, is dictated by statute. Therefore, expert guidance through the process is needed by most PI teams.**

SMEX Kickoff Meeting SR&QA Handout

- **The SMEX SR&QA Requirements document addresses Missions of Opportunity.**
  - **Permits further tailoring for Missions of Opportunity.**
  - **Shuttle proposers should refer to EPL Ref #25 (a) for System Safety scope & resulting cost planning.**
- **Specifics of PI SR&QA Program to be negotiated with Explorers during definition phase.**
  - **SMEX SR&QA Requirements are basis for PI SR&QA Program & associated documentation.**
  - **PI program shall be modeled after ANSI/ASQC Q9001-1994.**
  - **Quality Manual or equivalent document to be reviewed by GSFC for comments during Phase B.**
- **SMEX SR&QA document Highlights:**
  - **Invokes Hi-Reliability Workmanship standards.**

SMEX Kickoff Meeting SR&QA Handout

- Strongly Urges flight Printed Wiring Board Coupon DPA by certified facility prior to population with flight EEE parts.
- Requires a PI Failure Reporting System for phase C/D/E.
- Lays out Design Review Requirements.
- Details specific System Safety program requirements and deliverables with process flow descriptions (EPL Ref. #25 a-d).
  - Magnitude of System Safety effort <u>must not be under-estimated</u>.
    - Allocate/identify roles & resources.
    - Start early.
  - GSFC can help in numerous ways.
- EEE Parts Selection criteria per GSFC 311-INST-001 or equal.
  - PI shall maintain and review Parts Lists with GSFC.
  - PI shall use an organized system to manage parts application, evaluation, and use.
    - Includes mandatory GIDEP Alert and NASA Advisory responses.

SMEX Kickoff Meeting SR&QA Handout

- **Materials and Processes program required as typical for GSFC sponsored missions.**
- **Reliability**
  - **Risk assessments made and mitigation strategies identified.**
  - **FMEA at Instrument to Spacecraft interface.**
- **Software**
  - **Code to be structured, error free, and maintainable.**
  - **Establish & document SW requirements, external interface specs, user guides.**
  - **Internal (peer) and external software design reviews.**
- **Verification**
  - **Verification/test program to ensure all mission requirements are met.**
  - **Documentation to include verification matrix, environments matrix, and test procedures.**

SMEX Kickoff Meeting SR&QA Handout

- **Emergent Themes Directed by NASA HQ since AO release:**
  - **Red Team Reviews.**
    - **Team expectations can exceed baseline review requirements.**
      - **Reviews w/ Extra, detailed questions.**
      - **RFA trail & Failure Report closures thoroughly checked by Red Team.**
    - **GSFC Policy has shifted to Code 301 Chaired Reviews for PI Missions.**
  - **Reliability Emphasis On:**
    - **Probabilistic Risk Assessment (PRA).**
    - **Fault Tree Analysis, etc.**
    - **FMEA @ <u>subsystem level</u>.**
      - **Identify all single string design features.**
      - **Failure Impacts/mitigation.**
  - **Tangible Continuous Risk Tracking & Management System.**
  - **Software IV&V.**
    - **Each mission evaluated for SW complexity/risk/need.**
    - **Determination of appropriate level of IV&V involvement via standardized criteria.**
- **Mission Success is GSFC Center Director's Ultimate Responsibility to NASA Administrator.**